

DNS, Forward Failure Error

IPWorks

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2017, 2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.



Contents

1	Introduction	1
1.1	Alarm Description	1
1.2	Prerequisites	2
2	Procedure	3
2.1	Solving Network Issues	3
2.2	Checking Target DNS Server Status	3





1 Introduction

This instruction concerns alarm handling.

1.1 Alarm Description

This alarm is issued when the error rate of the recursive query that DNS forwards to another DNS server exceeds a given threshold (defined by attribute `thresholdHigh`) in a given time interval (defined by attribute `granularityPeriod`).

This alarm is cleared automatically when the error rate is below the given threshold (defined by attribute `thresholdLow`) in the given time interval (defined by attribute `granularityPeriod`).

Note: The attributes `thresholdHigh`, `thresholdLow`, and `granularityPeriod` are defined by the related MO `PmJob`.

The possible alarm causes and the corresponding fault reasons, fault locations, and impacts are described in Table 1.

Table 1 Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact	Solution
Network error	DNS server cannot get response in a given time interval.	Network is down.	Network	DNS server cannot get response from another DNS server.	See Section 2.1 on page 3
Target DNS server is down	Target DNS server cannot work properly.	Target DNS server is down.	Target DNS server	Certain DNS query cannot be disposed.	See Section 2.2 on page 3

Note: An alarm can appear as a result of the maintenance activity.

The alarm attributes are listed and explained in Table 2.

Table 2 Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	851973
Managed Object Class	ipworksDns



Attribute Name	Attribute Value
Source	ManagedElement=<Node Name>,SystemFunctions=1,Pm=1,PmJob=<PMJob name, the default PMJob is DnsForwardDefaultJob>,MeasurementReader=mr_1:<Hostname>
Specific Problem	DNS, Forward Failure Error
Event Type	qualityOfServiceAlarm(11)
Probable Cause	x733ThresholdCrossed(351)
Additional Text	The alarm is raised when the error rate of the queries that DNS forwards to another DNS server for recursive query exceeds the threshold in the given time interval (both defined by the related PMJob).;uuid:<Product_UUID> ⁽¹⁾
Perceived Severity	Warning

(1) <Product_UUID> is the universally unique identifier (UUID) of machine that generates the alarm. The value can be fetched from /sys/devices/virtual/dmi/id/product_uuid on the PL node.

1.2 Prerequisites

This section provides information on the documents, tools, and conditions that apply to the procedure.

1.2.1 Documents

Before starting this procedure, ensure that you have read the following documents:

- System Safety Information
- Personal Health and Safety Information
- Fault Management

1.2.2 Tools

No tools are required.

1.2.3 Conditions

No conditions.



2 Procedure

This section describes the procedure to follow when this alarm is received.

2.1 Solving Network Issues

To clear the alarm, do the following:

1. Check the network. If the network is down, then restore the network.
2. Confirm that the alarm has ceased. If the alarm remains, consult the next level of maintenance support. Further actions are outside the scope of this instruction.

2.2 Checking Target DNS Server Status

To clear the alarm, do the following:

1. Check the status of the target DNS server by using dig command. For example:

```
# dig @<Target DNS Server Traffic IP Address> <Arecord>
```

2. If the target DNS server is IPWorks DNS server, follow the steps below. Otherwise, resolve the problem on the target DNS server, further actions are outside of the scope of this instruction.
3. Log on to SC-1 or SC-2.

```
#ssh <Username>@<SC-1 or SC-2 IP Address>  
Password: <Password>
```

4. Check whether the DNS service is started. For example:

```
#ipw-ctr status dns <PL hostname>
```

5. If the DNS service is not started, issue the following command to start the DNS service:

```
#ipw-ctr start dns <PL hostname>
```

6. Confirm that the alarm has ceased. If the alarm remains, consult the next level of maintenance support. Further actions are outside the scope of this instruction.